

THE p -ADIC VALUATIONS OF WEIL SUMS OF BINOMIALS

DANIEL J. KATZ, PHILIPPE LANGEVIN, SANGMAN LEE,
AND YAKOV SAPOZHNIKOV

ABSTRACT. We investigate the p -adic valuation of Weil sums of the form $W_{F,d}(a) = \sum_{x \in F} \psi(x^d - ax)$, where F is a finite field of characteristic p , ψ is the canonical additive character of F , the exponent d is relatively prime to $|F^\times|$, and a is an element of F . Such sums often arise in arithmetical calculations and also have applications in information theory. For each F and d one would like to know $V_{F,d}$, the minimum p -adic valuation of $W_{F,d}(a)$ as a runs through the elements of F . We exclude exponents d that are congruent to a power of p modulo $|F^\times|$ (degenerate d), which yield trivial Weil sums. We prove that $V_{F,d} \leq (2/3)[F: \mathbb{F}_p]$ for any F and any nondegenerate d , and prove that this bound is actually reached in infinitely many fields F . We also prove some stronger bounds that apply when $[F: \mathbb{F}_p]$ is a power of 2 or when d is not congruent to 1 modulo $p-1$, and show that each of these bounds is reached for infinitely many F .

1. INTRODUCTION

We consider Weil sums of binomials of the form

$$(1) \quad W_{F,d}(a) = \sum_{x \in F} \psi(x^d - ax),$$

where F is a finite field, the exponent d is a positive integer such that $\gcd(d, q-1) = 1$, the coefficient a is in F , and $\psi: F \rightarrow \mathbb{C}$ is the canonical additive character of F . Throughout this paper, F is always a finite field of characteristic p and order $q = p^n$. Then $\psi(x) = e^{2\pi i \operatorname{Tr}(x)/p}$, where the absolute trace $\operatorname{Tr}: F \rightarrow \mathbb{F}_p$ is given by $\operatorname{Tr}(x) = x + x^p + \cdots + x^{p^{n-1}}$. The condition on d makes $x \mapsto x^d$ a permutation of F , which means that $W_{F,d}(0) = 0$. Every character sum of the more general form

$$\sum_{x \in F} \psi(bx^s + cx^t)$$

with $b \in F^\times$, $c \in F$, and $\gcd(s, q-1) = \gcd(t, q-1) = 1$ is equal to $W_{F,s/t}(-cb^{-t/s})$ via the reparameterization $y = b^{t/s}x^t$, where division signifies inversion modulo $q-1$. These sums and their close relatives arise often

Date: first version: 13 August 2016; this version: 20 March 2017.

The work of Katz, Lee, and Sapozhnikov on this paper was supported in part by the National Science Foundation under Grant DMS 1500856.

in number theory [8, 9, 11, 12, 13, 14, 22, 30, 31, 32, 43]. For example, the Kloosterman sum $\sum_{x \in F^\times} \psi(x^{-1} + ax)$ is $-1 + W_{F,|F|-2}(-a)$. Our Weil sums in (1) are also of practical interest, as they determine the performance of protocols in communications theory, remote sensing, cryptography, and coding theory. See the Appendix of [26] for how these sums relate to correlation of sequences and nonlinearity of boolean functions.

We are interested in the p -adic valuation of $W_{F,d}(a)$. We extend the p -adic valuation val_p from \mathbb{Q} to $\mathbb{Q}(e^{2\pi i/p})$ so that $\text{val}_p(1 - e^{2\pi i/p}) = 1/(p-1)$. Since $W_{F,d}(a)$ always lies in $\mathbb{Q}(e^{2\pi i/p})$, we see that its valuation must be an integer multiple of $1/(p-1)$. Bounds on the p -adic valuation of $W_{F,d}(a)$ have proved very helpful in determining the values of $W_{F,d}(a)$, as can be seen in [1, 2, 3, 4, 5, 6, 7, 10, 15, 16, 20, 21, 24, 26, 27, 28, 29, 34, 36, 37, 40, 41]. The main tool in determining the p -adic valuation of these Weil sums is Stickelberger's Theorem on the valuation of Gauss sums, which allows for an exact determination of

$$(2) \quad V_{F,d} = \min_{a \in F} \text{val}_p(W_{F,d}(a))$$

in terms of a combinatorial formula that is given in Lemma 2.9 below.

When d is a power of p modulo $q-1$, we see that

$$(3) \quad W_{F,d}(a) = \sum_{x \in F} \psi((1-a)x) = \begin{cases} |F| & \text{if } a = 1, \\ 0 & \text{otherwise,} \end{cases}$$

and $V_{F,d} = [F: \mathbb{F}_p]$. We say that d is *degenerate over F* in this case because $W_{F,d}$ degenerates to the Weil sum of a monomial or a constant. If d is degenerate over F , then it is also degenerate over any subfield of F . Since $\sum_{a \in F} W_{F,d}(a) = |F|$ (see [27, Corollary 2.6(i)]), the case where d is degenerate gives the highest possible value of $V_{F,d}$. In examining computer calculations of many values of $W_{F,d}(a)$ (see [35]), we noticed that there is a significant gap between the highest values of $V_{F,d}$ observed for nondegenerate d and the value $V_{F,d} = [F: \mathbb{F}_p]$ for degenerate d . This observation led us to conjecture that $V_{F,d} \leq (2/3)[F: \mathbb{F}_p]$ for nondegenerate d , and the main result of this paper is a proof of our conjecture. We also obtain stronger bounds in specific cases. One should note that nondegenerate d do not exist when $F = \mathbb{F}_2, \mathbb{F}_3$, or \mathbb{F}_4 .

Theorem 1.1. *Let $W_{F,d}(a)$ and $V_{F,d}$ be as defined in (1) and (2), where $\gcd(d, q-1) = 1$.*

- (i) *If d is degenerate over F , then $V_{F,d} = [F: \mathbb{F}_p]$.*
- (ii) *If d is nondegenerate over F , but is degenerate over \mathbb{F}_p , and*
 - (a) *if $[F: \mathbb{F}_p]$ is a power of 2, then $V_{F,d} \leq \frac{1}{2}[F: \mathbb{F}_p]$, but*
 - (b) *otherwise $V_{F,d} \leq \frac{2}{3}[F: \mathbb{F}_p]$.*
- (iii) *If d is nondegenerate over \mathbb{F}_p (so $p \geq 5$), and*
 - (a) *if $p \equiv 1 \pmod{4}$ and if $[F: \mathbb{F}_p]$ is odd, then $V_{F,d} \leq \frac{1}{2}[F: \mathbb{F}_p]$, but*
 - (b) *otherwise $V_{F,d} \leq \frac{1}{p-1} \lceil \frac{p-1}{3} \rceil [F: \mathbb{F}_p]$.*

One can see that when d is not degenerate over F , the bound $V_{F,d} \leq (2/3)[F:\mathbb{F}_p]$ is always true: this universal bound is proved in Theorem 3.1. The stronger bound in part (iia) when $[F:\mathbb{F}_p]$ is a power of 2 is proved in Theorem 4.1. Interestingly, these two proofs do not use Stickelberger's Theorem, which is the most commonly used tool in determining the p -divisibility of these sums. We do use Stickelberger's Theorem to establish the bounds in part (iii) (proved in Theorem 5.1). Part (i) follows from (3).

Remark 1.2. The compositum of parts (iia) and (iii) of Theorem 1.1 show that if $[F:\mathbb{F}_p]$ is a power of 2 and d is nondegenerate over F , then $V_{F,d} \leq (1/2)[F:\mathbb{F}_p]$.

Remark 1.3. For each case in Theorem 1.1 where we have an upper bound for $V_{F,d}$, we now mention those F covered by that case where we know that there exists an exponent d such that d meets the conditions of that case and $V_{F,d}$ equals the upper bound.

- For every field in case (iia) (see Lemma 4.2 in conjunction with Theorem 4.1).
- In case (iib), if $3 \mid [F:\mathbb{F}_p]$ (see Lemma 3.2).
- For every field in case (iia) (see Lemma 5.5).
- In case (iiib), if
 - $p \equiv 1 \pmod{3}$ and $3 \nmid [F:\mathbb{F}_p]$ (see Lemmata 5.6 and 5.7); or
 - $p \equiv 2 \pmod{3}$ and $2 \nmid [F:\mathbb{F}_p]$ (see Lemma 5.8).

This paper is organized as follows. After reviewing some basic results in Section 2, we prove the universal bound $V_{F,d} \leq (2/3)[F:\mathbb{F}_p]$ (when d is nondegenerate over F) in Section 3, and then show that this bound is attained whenever $[F:\mathbb{F}_p]$ is divisible by 3. In Section 4 we prove the bound in part (iia) of Theorem 1.1, where F is obtained from its prime subfield via a tower of quadratic extensions. In Section 4 we also prove that this bound is always attained for some d in every field F satisfying the hypotheses. The bounds in part (iii) of Theorem 1.1, when d is known to be nondegenerate over the prime subfield, are proved in Section 5. In Section 6, we discuss some open problems.

2. PRELIMINARIES

Here we recall some well known results that will be useful in the rest of the paper. We continue to use the definition of the Weil sum $W_{F,d}(a)$ from (1) and the definition $V_{F,d}$ from (2) in this section and in the rest of the paper.

Remark 2.1. If d is an integer coprime to $q-1$, then $(-1)^d = -1$ in F . This is because the coprimality makes d odd when p is odd.

Remark 2.2. If d and d' are positive integers coprime to $q-1$ such that $d' \equiv dp^k \pmod{q-1}$ for some $k \in \mathbb{Z}$, then $W_{F,d'}(a) = W_{F,d}(a)$ for all $a \in F$. This is because for every $x \in F$, we have $x^q = x$ and also the

absolute trace has $\text{Tr}(x^p) = \text{Tr}(x)$, so that the canonical additive character has $\psi(x^p) = \psi(x)$.

Remark 2.3. If d and e are positive integers coprime to $q - 1$ with $de \equiv 1 \pmod{q - 1}$, then $W_{F,e}(a) = W_{F,d}(a^{-e})$ for every $a \in F^\times$ via the reparameterization mentioned in the Introduction (and use Remark 2.1 to get the correct sign). Since $W_{F,d}(0) = W_{F,e}(0) = 0$, and $a \mapsto a^{-e}$ is a permutation of F^\times , this means that $V_{F,e} = V_{F,d}$.

Remark 2.4. If d is a positive integer with $\gcd(d, q - 1) = 1$, then it is easy to calculate that $\sum_{a \in F} W_{F,d}(a) = q$ (the first power moment: see [27, Corollary 2.6(i)]), so $V_{F,d} \leq \text{val}_p(q) = [F: \mathbb{F}_p]$. And the inequality becomes an equality if d is degenerate over F by (3).

We let $\widehat{F^\times}$ denote the group of multiplicative characters of F , and we denote the trivial multiplicative character by 1 and use the shorthand $\bar{\chi} = \chi^{-1}$. For $\chi \in \widehat{F^\times}$, we define the Gauss sum

$$\tau(\chi) = \sum_{a \in F^\times} \psi(a) \chi(a),$$

where ψ is the canonical additive character of F as defined in the Introduction. We extend the p -adic valuation val_p from \mathbb{Q} to $\mathbb{Q}(e^{2\pi i/p}, e^{2\pi i/(q-1)})$ so that $\text{val}_p(1 - e^{2\pi i/p}) = 1/(p - 1)$. This enables us to consider the p -adic valuation of our Gauss sums.

Lemma 2.5. *Let d be a positive integer with $\gcd(d, q - 1) = 1$. Then for $a \in F^\times$, we have*

$$W_{F,d}(a) = \frac{q}{q-1} + \frac{1}{q-1} \sum_{\substack{\chi \in \widehat{F^\times} \\ \chi \neq 1}} \tau(\chi) \tau(\bar{\chi}^d) \chi^d(a),$$

and for $\chi \in \widehat{F^\times}$, we have

$$\sum_{a \in F^\times} W_{F,d}(a) \bar{\chi}^d(a) = \begin{cases} q & \text{if } \chi = 1, \\ \tau(\chi) \tau(\bar{\chi}^d) & \text{otherwise.} \end{cases}$$

Proof. The first formula is proved in [2, eq. (3)], and the second is easily obtained from eq. (4) of the same paper. \square

Corollary 2.6. *Let d be a positive integer with $\gcd(d, q - 1) = 1$. If $q = 2$, then d is degenerate over F and $V_{F,d} = 1$. If $q > 2$, then*

$$V_{F,d} = \min_{\substack{\chi \in \widehat{F^\times} \\ \chi \neq 1}} \text{val}_p(\tau(\chi) \tau(\bar{\chi}^d)).$$

Proof. The $q = 2$ case is immediate from Remark 2.4, so assume $q > 2$ henceforth. Note that multiplicative characters take nonzero elements of F

to roots of unity in \mathbb{C} , which have p -adic valuation 0. Thus the first formula in Lemma 2.5 shows that

$$\min_{a \in F^\times} \text{val}_p(W_{F,d}(a)) \geq \min \left(\{\text{val}_p(q)\} \cup \{\text{val}_p(\tau(\chi)\tau(\bar{\chi}^d)) : \chi \in \widehat{F^\times}, \chi \neq 1\} \right),$$

and the reverse inequality follows from the second formula in Lemma 2.5. (In essence, the minimum p -adic valuation of the Fourier coefficients is the same as the minimum p -adic valuation of the original function when p does not divide the order of the underlying group.) Since $W_{F,d}(0) = 0$, we could extend the minimization on the left hand side to include $a = 0$. Thus

$$V_{F,d} = \min \left(\{\text{val}_p(q)\} \cup \{\text{val}_p(\tau(\chi)\tau(\bar{\chi}^d)) : \chi \in \widehat{F^\times}, \chi \neq 1\} \right).$$

So it remains to show that there is some nontrivial $\chi \in \widehat{F^\times}$ such that $\text{val}_p(\tau(\chi)\tau(\bar{\chi}^d)) \leq \text{val}_p(q)$. Since $|\tau(\chi)|^2 = q$ for any nontrivial multiplicative character and $\tau(\bar{\chi}) = \chi(-1)\overline{\tau(\chi)}$ (see [38, Theorems 5.11, 5.12(iii)]), and since d is coprime to $q-1$, we see that $\prod_{\chi \neq 1} \tau(\chi)\tau(\bar{\chi}^d) \in \{\pm q^{q-2}\}$. So there is some nontrivial $\chi \in \widehat{F^\times}$ with $\text{val}_p(\tau(\chi)\tau(\bar{\chi}^d)) \leq \text{val}_p(q)$. \square

We also state some useful bounds relating $V_{F,d}$ and $V_{K,d}$ when K is a subfield of F .

Lemma 2.7. *Let K be a subfield of F , and let d be a positive integer with $\gcd(d, |F^\times|) = 1$. Then $V_{K,d} \leq V_{F,d} \leq [F:K] \cdot V_{K,d}$.*

Proof. First we prove the lower bound on $V_{F,d}$. Let ψ_K and ψ_F be the canonical additive characters for K and F , respectively, and note that $\psi_F = \psi_K \circ \text{Tr}_{F/K}$, where $\text{Tr}_{F/K}$ is the Galois-theoretic relative trace from F to K . Let R be a set of representatives for the cosets of K^\times in F^\times . Then for any $a \in K$, we have

$$\begin{aligned} W_{F,d}(a) &= 1 + \sum_{x \in F^\times} \psi_F(x^d - ax) \\ &= 1 + \sum_{r \in R} \sum_{y \in K^\times} \psi_K(\text{Tr}_{F/K}((ry)^d - ary)) \\ &= 1 - |R| + \sum_{r \in R} \sum_{y \in K} \psi_K(\text{Tr}_{F/K}(r^d)y^d - \text{Tr}_{F/K}(ar)y). \end{aligned}$$

Now let us consider the values taken on by the inner sum over K in the last expression: these depend on whether the coefficients $\text{Tr}_{F/K}(r^d)$ and $\text{Tr}_{F/K}(ar)$ are zero or not. If both coefficients are zero, the sum is $|K|$, and if only one is zero, then the sum is 0: since $\gcd(d, |F^\times|) = 1$, the map $y \mapsto y^d$ is a permutation of F , and thus restricts to a permutation of K . If both coefficients are nonzero, then the reparameterization described in the Introduction shows that the inner sum over K is $W_{K,d}(b)$ for some $b \in K$. Since $V_{K,d} \leq [K:\mathbb{F}_p] = \text{val}_p(|K|)$ by Remark 2.4, we see that our inner sum always has a p -adic valuation of at least $V_{K,d}$. Also note that $|R| = (|F| - 1)/(|K| - 1)$, so that $|R| - 1$ is a multiple of $|K|$, and so it also

has a p -adic valuation greater than or equal to $V_{K,d}$. So for any $a \in F$, we see that $W_{F,d}(a)$ has a p -adic valuation greater than or equal to $V_{K,d}$, so $V_{F,d} \geq V_{K,d}$.

Now we prove the upper bound on $V_{F,d}$. If d is degenerate over K , then Remark 2.4 shows that $[F: K] \cdot V_{K,d} = [F: \mathbb{F}_p]$, and so our upper bound is true by another application of Remark 2.4. So from now on we assume that d is nondegenerate over K (which forces $|K| > 2$). Let $N_{F/K}$ denote the Galois-theoretic relative norm from K to F . Then the Davenport-Hasse relation [38, Theorem 5.14] tells us that for $\chi \in \widehat{K^\times}$, we have

$$-\tau(\chi \circ N_{F/K}) = (-\tau(\chi))^{[F: K]}.$$

As χ runs through the nontrivial characters in $\widehat{K^\times}$, their lifts $\chi \circ N_{F/K}$ run through the nontrivial characters in $\widehat{F^\times}$ whose orders are divisors of $|K^\times|$. So Corollary 2.6 and the Davenport-Hasse relation show us that

$$\begin{aligned} V_{F,d} &\leq \min_{\substack{\chi \in \widehat{K^\times} \\ \chi \neq 1}} \text{val}_p(\tau(\chi \circ N_{F/K}) \tau((\chi \circ N_{F/K})^d)) \\ &= \min_{\substack{\chi \in \widehat{K^\times} \\ \chi \neq 1}} [F: K] \text{val}_p(\tau(\chi) \tau(\bar{\chi}^d)) \\ &= [F: K] \cdot V_{K,d}. \end{aligned} \quad \square$$

Remark 2.8. The special case of Lemma 2.7 for characteristic 2 was proved in [7, Theorem 7.1] using McEliece's Theorem on 2-divisibility of weights of words in cyclic codes (see [39, Corollary to Theorem 2]), which is closely related to Stickelberger's Theorem. Note that our proof in this paper of the general case uses neither Stickelberger's nor McEliece's Theorem.

Now we provide the definitions needed to make use of Stickelberger's Theorem. If t is an integer with $t \geq 2$ and n is a positive integer, and if $a \in \mathbb{Z}/(t^n - 1)\mathbb{Z}$, we define the *standard t -ary expansion of a* to be the expression

$$a = a_0 t^0 + a_1 t^1 + \cdots + a_{n-1} t^{n-1},$$

where the powers of t are elements of $\mathbb{Z}/(t^n - 1)\mathbb{Z}$ and a_0, \dots, a_{n-1} are elements of \mathbb{Z} with $0 \leq a_i < t$ for every i , and where we insist that $a_0 = \cdots = a_n = 0$ when $a = 0$ (to make the a_i 's uniquely defined). Then we define the *t -ary weight of $a \in \mathbb{Z}/(t^n - 1)\mathbb{Z}$* ,

$$(4) \quad \text{wt}_{t,n}(a) = a_0 + a_1 + \cdots + a_{n-1},$$

so that $\text{wt}_{t,n}: \mathbb{Z}/(t^n - 1)\mathbb{Z} \rightarrow \mathbb{Z}$ with $0 \leq \text{wt}_{t,n}(a) < n(t - 1)$ for every $a \in \mathbb{Z}/(t^n - 1)\mathbb{Z}$. Note that our weight function is subadditive, that is, $\text{wt}_{t,n}(a + b) \leq \text{wt}_{t,n}(a) + \text{wt}_{t,n}(b)$ for all $a, b \in \mathbb{Z}/(t^n - 1)\mathbb{Z}$. And this inequality becomes an equality if and only if there are no carries (and no cyclic carries from the $(n - 1)$ th digit to the 0th digit) when we compute the sum of a and b in base t arithmetic by summing their standard t -ary expansions.

Lemma 2.9. *Let $q = p^n > 2$, and let d be a positive integer with $\gcd(d, q - 1) = 1$. Let*

$$m = \min_{\substack{a \in \mathbb{Z}/(p^n-1)\mathbb{Z} \\ a \neq 0}} \text{wt}_{p,n}(a) + \text{wt}_{p,n}(-da),$$

or equivalently,

$$m = n(p-1) + \min_{\substack{a \in \mathbb{Z}/(p^n-1)\mathbb{Z} \\ a \neq 0}} \text{wt}_{p,n}(da) - \text{wt}_{p,n}(a).$$

Then $V_{F,d} = m/(p-1)$.

Proof. One can see that our two definitions of m are equivalent by reparameterizing the first one with $-a$ in place of a and then noting that for any nonzero $a \in \mathbb{Z}/(p^n-1)\mathbb{Z}$, we have $\text{wt}_{p,n}(-a) = n(p-1) - \text{wt}_{p,n}(a)$. Now let $\zeta = e^{2\pi i/(q-1)}$, and identify F with $\mathbb{Z}[\zeta]/P$, where P is a prime ideal of $\mathbb{Z}[\zeta]$ containing p . Then $\zeta + P$ is a primitive element of F . Let $\omega: F^\times \rightarrow \mathbb{Q}(\zeta)$ be the Teichmüller character, which is determined by $\omega(\zeta + P) = \zeta$. Then Stickelberger's Theorem [33, Theorem 2.1] says that $\text{val}(\tau(\omega^{-a})) = \text{wt}_{p,n}(a)/(p-1)$ for every $a \in \mathbb{Z}/(p^n-1)\mathbb{Z}$. And ω^{-a} runs through the nontrivial multiplicative characters of F as a runs through the nonzero elements of $\mathbb{Z}/(p^n-1)\mathbb{Z}$, so the expression for $V_{F,d}$ in Corollary 2.6 becomes the desired expression. \square

Corollary 2.10. *Let d be a positive integer with $\gcd(d, q-1) = 1$. Then $V_{F,d} = [F: \mathbb{F}_p]$ if and only if d is degenerate over F . If d is nondegenerate over F , then $2/(p-1) \leq V_{F,d} < [F: \mathbb{F}_p]$ and $V_{F,d} = 2/(p-1)$ if and only if $-d$ is congruent to a power of p modulo $q-1$.*

Proof. Remark 2.4 handles the degenerate case. So we suppose d is nondegenerate over F , which forces $q = p^n > 4$.

For the upper bound, look at the formula for m in Lemma 2.9. Since d is not a power of p modulo $\mathbb{Z}/(p^n-1)\mathbb{Z}$, we see that $\text{wt}_{p,n}(-d) < n(p-1) - 1$, and then $m \leq \text{wt}_{p,n}(1) + \text{wt}_{p,n}(-d) < n(p-1)$. Thus by Lemma 2.9, we know that $V_{F,d} < n = [F: \mathbb{F}_p]$.

In the formula for m in Lemma 2.9, note that a is nonzero and d is coprime to p^n-1 , so both $\text{wt}_{p,n}(a)$ and $\text{wt}_{p,n}(-da)$ are always strictly positive integers. And these weights are both equal to 1 simultaneously if and only if both a and $-da$ are powers of p modulo $q-1$, which will occur for some $a \in \mathbb{Z}/(q-1)\mathbb{Z}$ if and only if $-d$ is a power of p modulo $q-1$. This proves our lower bound and shows us when it is achieved. \square

Corollary 2.11. *Let d be a positive integer with $\gcd(d, q-1) = 1$. Then $V_{F,d} + V_{F,-d} \leq [F: \mathbb{F}_p] + \frac{2}{p-1}$.*

Proof. If $q = 2$, then both d and $-d$ are degenerate over F , and then our inequality follows from Corollary 2.10, so assume $q > 2$ henceforth.

By Lemma 2.9, we know that $(p-1)V_{F,d} \leq 1 + \text{wt}_{p,n}(-d)$ and $(p-1)V_{F,-d} \leq 1 + \text{wt}_{p,n}(d)$. So $(p-1)(V_{F,d} + V_{F,-d}) \leq 2 + \text{wt}_{p,n}(d) + \text{wt}_{p,n}(-d)$.

Since d is coprime to $q - 1$ and $q > 2$, we see that d must be nonzero modulo $q - 1$, and so $\text{wt}_{p,n}(d) + \text{wt}_{p,n}(-d) = n(p - 1)$. Thus $V_{F,d} + V_{F,-d} \leq n + 2/(p - 1)$. \square

3. PROOF OF THE UNIVERSAL UPPER BOUND

In this section, we prove an upper bound on $V_{F,d}$ that holds whenever d is nondegenerate over F , and then show that our bound is attained for infinitely many fields F .

Theorem 3.1. *If F is a finite field of characteristic p and order q , and d is a positive integer with $\gcd(d, q - 1) = 1$ such that d is not degenerate over F , then $V_{F,d} \leq \frac{2}{3}[F : \mathbb{F}_p]$.*

Proof. Let $\psi : F \rightarrow \mathbb{C}$ be the canonical additive character of F , and for $u, a \in F$, define

$$S_{u,a} = \sum_{x \in F} \psi(ux^d - ax).$$

Then for $u, v, w, a \in F$, we have

$$\begin{aligned} \frac{1}{q} \sum_{a \in F} S_{u,a} S_{v,a} S_{w,a} &= \frac{1}{q} \sum_{r,s,t,a \in F} \psi(ur^d + vs^d + wt^d) \psi(-a(r + s + t)) \\ &= \sum_{\substack{r,s,t \in F \\ r+s+t=0}} \psi(ur^d + vs^d + wt^d) \\ &= \sum_{\substack{r,s \in F \\ r+s=0}} \psi(ur^d + vs^d) + \sum_{\substack{r,s \in F \\ t \in F^\times \\ r+s=-t}} \psi(ur^d + vs^d + wt^d) \\ &= \sum_{r \in F} \psi((u - v)r^d) + \sum_{\substack{x,y \in F \\ t \in F^\times \\ x+y=-1}} \psi((ux^d + vy^d + w)t^d) \\ &= q\delta_{u,v} - q + \sum_{\substack{x,y,t \in F \\ x+y=-1}} \psi((ux^d + vy^d + w)t^d), \end{aligned}$$

where δ is the Kronecker delta, and where the first sum in the fourth step is obtained using Remark 2.1, while the second sum in the fourth step is obtained via the reparameterization $(r, s) = (tx, ty)$.

For $u, v, w \in F$, we define $N(u, v, w)$ to be the number of $(x, y) \in F^2$ simultaneously satisfying $x + y = -1$ and $ux^d + vy^d = -w$, and we define $f_{v,u}(x) = v(x + 1)^d - ux^d$. Then

$$\begin{aligned} N(u, v, w) &= \left| \left\{ (x, y) \in F^2 : x + y = -1, ux^d + vy^d = -w \right\} \right| \\ &= |\{x \in F : f_{v,u}(x) = w\}|. \end{aligned}$$

Since our assumption that $\gcd(d, q-1) = 1$ makes $t \mapsto t^d$ a permutation of F , our calculation in the previous paragraph shows that

$$\sum_{a \in F} S_{u,a} S_{v,a} S_{w,a} = q^2 (\delta_{u,v} - 1 + N(u, v, w)).$$

If we could find $u, v, w \in F$ with $u \neq v$ and $p \mid N(u, v, w)$, then we would have $p \nmid (\delta_{u,v} - 1 + N(u, v, w))$, and so

$$\text{val}_p \left(\sum_{a \in F} S_{u,a} S_{v,a} S_{w,a} \right) = 2[F: \mathbb{F}_p],$$

which would imply that $\text{val}_p(S_{b,a}) \leq 2[F: \mathbb{F}_p]/3$ for some $(b, a) \in F^2$, and in fact, this must be true for some $b \in F^\times$ because direct calculation from the definition of $S_{u,a}$ shows that

$$S_{0,a} = \begin{cases} q & \text{if } a = 0, \\ 0 & \text{otherwise,} \end{cases}$$

so that $\text{val}_p(S_{0,a}) \geq [F: \mathbb{F}_p]$ for all $a \in F$. And when $b \neq 0$, then $S_{b,a} = W_{F,d}(b^{-1/d}a)$ (where $1/d$ signifies the multiplicative inverse of d modulo $q-1$), so this would prove our claim.

Since $N(u, v, w)$ counts the zeroes of a polynomial, it is always a nonnegative integer. For any $(u, v) \in F^2$, we observe that

$$\sum_{w \in F} N(u, v, w) = q.$$

So the only way that we can have $p \nmid N(u, v, w)$ for every $w \in F$ is if $N(u, v, w) = 1$ for every $w \in F$, and this is true if and only if $x \mapsto f_{v,u}(x)$ is a permutation of F . So we will have completed our proof if we can find some $u, v \in F$ with $u \neq v$ such that $x \mapsto f_{v,u}(x)$ is not a permutation of F . In fact, we shall show that for every $v \in F^\times$, there is some $u \in F \setminus \{v\}$ such that $x \mapsto f_{v,u}(x)$ is not a permutation of F .

Let $v \in F^\times$, and suppose that $x \mapsto f_{v,u}(x)$ is a permutation of F for every $u \in F \setminus \{v\}$ in order to show a contradiction. Thus for any $u, x, y \in F$ with $u \neq v$ and $x \neq y$, we have $f_{v,u}(x) \neq f_{v,u}(y)$, and thus

$$\frac{f_{v,0}(y) - f_{v,0}(x)}{y^d - x^d} \neq u,$$

where we have used the fact that $x^d \neq y^d$ because $z \mapsto z^d$ is a permutation of F . So we must have

$$\frac{f_{v,0}(y) - f_{v,0}(x)}{y^d - x^d} = v,$$

for every $x, y \in F$ with $x \neq y$. This means that $x \mapsto f_{v,v}(x)$ is a constant function on F , and in fact, the constant must be v since $f_{v,v}(0) = v$. Since $v \neq 0$, this means that the function $x \mapsto f_{1,1}(x) - 1 = (x+1)^d - x^d - 1$ must be the zero function on F . Let d' be the least positive integer congruent to d

modulo $q-1$, and write $d' = p^k e$ for some nonnegative integer k and positive integer e with $p \nmid e$. So $d \equiv p^k e \pmod{q-1}$ with $0 < e < q$, and in fact $e > 1$ because d is nondegenerate over F . For any $x \in F$, we have $x^d = x^{p^k e}$, so that $0 = f_{1,1}(x) - 1 = (x+1)^{p^k e} - x^{p^k e} - 1 = ((x+1)^e - x^e - 1)^{p^k}$, so that $x \mapsto (x+1)^e - x^e - 1$ is the zero function on F . But

$$(x+1)^e - x^e - 1 = ex^{e-1} + \sum_{j=1}^{e-2} \binom{e}{j} x^j,$$

and since $p \nmid e$, this is a polynomial of degree $e-1$ with $0 < e-1 < q$, and so is not divisible by $x^q - x$, so that $x \mapsto (x+1)^e - x^e - 1$ is not the zero function on F . This contradiction shows that $f_{v,u}(x)$ is not a permutation of F for some $u \in F \setminus \{v\}$, which completes our proof. \square

The following result shows that infinitely many fields F have some exponent d such that the upper bound in Theorem 3.1 is attained.

Lemma 3.2. *Suppose that $[F : \mathbb{F}_p]$ is not a power of 2. Let ℓ be the smallest odd prime divisor of $[F : \mathbb{F}_p]$. Then there is some d with $\gcd(d, q-1) = 1$ such that d is nondegenerate over F but degenerate over \mathbb{F}_p and $V_{F,d} = \frac{\ell+1}{2\ell}[F : \mathbb{F}_p]$.*

Proof. Recall that $n = [F : \mathbb{F}_p]$. If $p = 2$, and $d = 2^{n/\ell} + 1$ or $d = 2^{2n/\ell} - 2^{n/\ell} + 1$, then it is known (see [17], [23, Theorem 5], [24, Remark 3], [25, Theorem 16], [44]) that $\{W_{F,d}(a) : a \in F\} = \{0, \pm \sqrt{2^{n(\ell+1)/\ell}}\}$, so $V_{F,d} = n(\ell+1)/(2\ell)$. If p is odd and $d = (p^{2n/\ell} + 1)/2$ or $d = p^{2n/\ell} - p^{n/\ell} + 1$, then it is known (see [18], [19, Theorem 4.9], [42, Theorems 3.3, 3.4]) that $\{W_{F,d}(a) : a \in F\} = \{0, \pm \sqrt{p^{n(\ell+1)/\ell}}\}$, so $V_{F,d} = n(\ell+1)/(2\ell)$.

Now we demonstrate that each of these exponents is coprime to the order of the group of units for its field. First of all, $\gcd(2^{n/\ell} + 1, 2^n - 1) = \gcd(2^{n/\ell} + 1, (-1)^\ell - 1) = \gcd(2^{n/\ell} + 1, -2) = 1$. And if p is odd, then $(p^{2n/\ell} + 1)/2$ is odd, so that

$$\begin{aligned} \gcd\left(\frac{p^{2n/\ell} + 1}{2}, p^n - 1\right) &= \frac{1}{2} \gcd(p^{2n/\ell} + 1, p^n - 1) \\ &= \frac{1}{2} \gcd(p^{2n/\ell} + 1, (-1)^{(\ell-1)/2} p^{n/\ell} - 1) \\ &= \frac{1}{2} \gcd(1 + 1, (-1)^{(\ell-1)/2} p^{n/\ell} - 1) \\ &= 1. \end{aligned}$$

Now we examine $d = p^{2n/\ell} - p^{n/\ell} + 1$ for an arbitrary prime p . We write the least odd prime divisor ℓ of n as $\ell = 3k + r$ with $k \in \mathbb{Z}$ and $r \in \{0, 1, 2\}$. Then $(p^{2n/\ell} - p^{n/\ell} + 1)(p^{n/\ell} + 1) = p^{3n/\ell} + 1$, so then $\gcd(p^{2n/\ell} - p^{n/\ell} + 1, p^n - 1) = \gcd(p^{2n/\ell} - p^{n/\ell} + 1, (-1)^k p^{rn/\ell} - 1)$. If $r = 0$, then $\ell = 3$, so then $k = 1$, and then our greatest common divisor is $\gcd(p^{2n/3} - p^{n/3} + 1, -2) = 1$. If $r = 1$,

then k must be even (no prime is 4 modulo 6), so then our greatest common divisor becomes $\gcd(p^{2n/\ell} - p^{n/\ell} + 1, p^{n/\ell} - 1) = \gcd(1 - 1 + 1, p^{n/\ell} - 1) = 1$. And if $r = 2$, then k must be odd (no odd prime is 2 modulo 6), so our greatest common divisor becomes $\gcd(p^{2n/\ell} - p^{n/\ell} + 1, -p^{2n/\ell} - 1) = \gcd(p^{n/\ell}, -p^{2n/\ell} - 1) = \gcd(p^{n/\ell}, -1) = 1$.

Since $V_{F,d} < [F : \mathbb{F}_p]$ for each of the four d proposed above, it is clear that these values of d are all nondegenerate over F . And our exponents are clearly degenerate over \mathbb{F}_p : all exponents are degenerate over \mathbb{F}_2 , and when p is odd, both $(p^{2n/\ell} + 1)/2 = 1 + (p^{n/\ell} - 1)(p^{n/\ell} + 1)/2$ and $p^{2n/\ell} - p^{n/\ell} + 1 = 1 + (p^{n/\ell} - 1)p^{n/\ell}$ are congruent to 1 modulo $p - 1$. \square

4. TOWERS OF QUADRATIC EXTENSIONS

In this section, we prove an upper bound for $V_{F,d}$ when the degree of F over its prime subfield \mathbb{F}_p is a power of 2, and when d is nondegenerate over F , but is degenerate over \mathbb{F}_p . (This is part (iia) of Theorem 1.1.) Then we show that for any such F , there is some such d for which our upper bound is attained.

Theorem 4.1. *Let $[F : \mathbb{F}_p] = 2^s$ for some $s \geq 1$. Let d be a positive integer with $\gcd(d, q - 1) = 1$ such that d is not degenerate over F , but is degenerate over \mathbb{F}_p . Then $V_{F,d} \leq \frac{1}{2}[F : \mathbb{F}_p]$, and this is always an equality if d is degenerate in the subfield of F of order \sqrt{q} .*

Proof. Let L be the smallest subfield of F (possibly equal to F) such that d is not degenerate over L , and let K be the unique subfield of L with $[L : K] = 2$. Then by [2, Corollary 4.4], we have $V_{L,d} = [K : \mathbb{F}_p]$. Lemma 2.7 then shows that $V_{F,d} \leq [F : L][K : \mathbb{F}_p] = \frac{1}{2}[F : \mathbb{F}_p]$. If d is degenerate in the subfield of F of order \sqrt{q} , then $L = F$, and so $V_{F,d} = V_{L,d} = [K : \mathbb{F}_p] = \frac{1}{2}[L : \mathbb{F}_p] = \frac{1}{2}[F : \mathbb{F}_p]$. \square

The following result shows that if F is as described in Theorem 4.1, then there is always an exponent d as described in the same theorem such that the upper bound on $V_{F,d}$ in the theorem is attained. Note that since there are no nondegenerate exponents over \mathbb{F}_2 , \mathbb{F}_3 , and \mathbb{F}_4 , we need to work with a field having more than four elements to satisfy the hypotheses of Theorem 4.1.

Lemma 4.2. *Let $q > 4$ and $[F : \mathbb{F}_p] = 2^s$ for some $s \geq 1$. Let K be the unique subfield of F of order \sqrt{q} . Then there is always some positive integer d with $\gcd(d, q - 1) = 1$ such that d is nondegenerate over F but degenerate over K . For examples of such d , we have*

- $d = q - \sqrt{q} - 1$ when $\sqrt{q} \pmod{3} \in \{0, 1\}$,
- $d = (q + 2)/3$ when $\sqrt{q} \pmod{9} \in \{2, 8\}$, and
- $d = (2q + 1)/3$ when $\sqrt{q} \pmod{9} \in \{5, 8\}$.

Proof. We prove this result by proving that the above examples satisfy the desired conditions.

First suppose $\sqrt{q} \pmod{3} \in \{0, 1\}$ and $d = q - \sqrt{q} + 1$. Note that $d \equiv 1 \pmod{\sqrt{q} - 1}$, so d is degenerate over K and $\gcd(d, \sqrt{q} - 1) = 1$. Also note that $\gcd(d, \sqrt{q} + 1) = \gcd(1 + 1 + 1, \sqrt{q} + 1) = 1$ since $3 \nmid \sqrt{q} + 1$. Thus $\gcd(d, q - 1) = 1$. Finally, note that $q/p < q - \sqrt{q} + 1 < q - 1$ because $q > 4$ so that it is clear that $d = q - \sqrt{q} + 1$ is not a power of p modulo $q - 1$. So d is nondegenerate over F .

Now suppose that $\sqrt{q} \pmod{9} \in \{2, 8\}$ and $d = (q + 2)/3$. Note that $3d \equiv 3 \pmod{\sqrt{q} - 1}$ and since $3 \nmid \sqrt{q} - 1$, this means that $d \equiv 1 \pmod{\sqrt{q} - 1}$, so d is degenerate over K . Also note that $\gcd(3d, q - 1) = \gcd(3, q - 1)$ but $3 \nmid d$, so $\gcd(d, q - 1) = 1$. If $p \geq 3$, then $q/p < (q + 2)/3 < q - 1$ because $q > 4$, so it is clear that $d = (q + 2)/3$ is not a power of p modulo $q - 1$. And if $p = 2$, then $q/4 < (q + 2)/3 < q/2 < q - 1$ because $q > 4$, so it is clear that $d = (q + 2)/3$ is not a power of p modulo $q - 1$. So d is nondegenerate over F .

Now suppose that $\sqrt{q} \pmod{9} \in \{5, 8\}$ and $d = (2q + 1)/3$. Note that $3d \equiv 3 \pmod{\sqrt{q} - 1}$ and since $3 \nmid \sqrt{q} - 1$, this means that $d \equiv 1 \pmod{\sqrt{q} - 1}$, so d is degenerate over K . Also note that $\gcd(3d, q - 1) = \gcd(3, q - 1)$ but $3 \nmid d$, so $\gcd(d, q - 1) = 1$. And $q/p < (2q + 1)/3 < q - 1$ because $q > 4$, so it is clear that $d = (2q + 1)/3$ is not a power of p modulo $q - 1$. So d is nondegenerate over F . \square

5. EXPONENTS THAT ARE NONDEGENERATE OVER THE PRIME SUBFIELD

In this section, we obtain upper bounds on $V_{F,d}$ when d is nondegenerate over the prime subfield \mathbb{F}_p of F . (This is part (iii) of Theorem 1.1.) Our results here also show that these upper bounds are attained in infinitely many of the fields under consideration: see Remark 1.3 for details. We prove our bounds in Theorem 5.1, which itself is based on a few other results (Propositions 5.2–5.4 and Lemma 5.5), which in turn are based on further technical results (Lemmata 5.6–5.8). To show the motivation for the various results, we present Theorem 5.1 first, then proceed to the intermediate results upon which our proof of Theorem 5.1 directly depends, and conclude with proofs of the tributary claims that we use to establish the intermediate results. The lemmata in this section also show that the upper bound in Theorem 5.1 is met infinitely often (cf. Remark 1.3).

Theorem 5.1. *Let d be a positive integer with $\gcd(d, q - 1) = 1$ and $d \not\equiv 1 \pmod{p - 1}$. If $d \equiv (p + 1)/2 \pmod{p - 1}$ (which can only happen if $p \equiv 1 \pmod{4}$) and if n is odd, then $V_{F,d} \leq \frac{1}{2}[F : \mathbb{F}_p]$. Otherwise $V_{F,d} \leq \frac{1}{p-1} \lceil \frac{p-1}{3} \rceil [F : \mathbb{F}_p]$.*

Proof. Our conditions on d imply that $p \geq 5$. If $d \not\equiv (p + 1)/2 \pmod{p - 1}$, then Propositions 5.2 and 5.3 below show that $V_{\mathbb{F}_p,d} \leq \frac{1}{p-1} \lceil \frac{p-1}{3} \rceil$, and Lemma 2.7 shows that $V_{F,d} \leq V_{\mathbb{F}_p,d} \cdot [F : \mathbb{F}_p]$, thus securing our bound.

So suppose $d \equiv (p + 1)/2 \pmod{p - 1}$ henceforth. We must have $p \equiv 1 \pmod{4}$, since otherwise d would be even, hence not coprime to $q - 1$.

By Lemma 5.5 below, we have $V_{\mathbb{F}_p, d} = 1/2$, and Lemma 2.7 shows that $V_{F, d} \leq V_{\mathbb{F}_p, d} \cdot [F : \mathbb{F}_p]$, thus securing the desired bound when n is odd, and also the desired bound when n is even and $p = 5$, since $\frac{1}{5-1} \lceil \frac{5-1}{3} \rceil = \frac{1}{2}$.

So suppose that n is even and $p > 5$ henceforth. Since $p \equiv 1 \pmod{4}$, this means that $p \geq 13$. So Proposition 5.4 below shows that $V_{\mathbb{F}_{p^2}, d} \leq 1/2$. Then we use Lemma 2.7 to see that $V_{F, d} \leq \frac{1}{2} [F : \mathbb{F}_{p^2}] = \frac{1}{4} [F : \mathbb{F}_p] < \frac{1}{p-1} \lceil \frac{p-1}{3} \rceil [F : \mathbb{F}_p]$. \square

Now we prove four results upon which our proof of Theorem 5.1 depends.

Proposition 5.2. *Let F be a prime field of order p with $p \equiv 1 \pmod{3}$. If d is a positive integer with $\gcd(d, p-1) = 1$ and $d \not\equiv 1 \pmod{(p-1)/2}$, then $V_{F, d} \leq 1/3$. Equality is achieved if and only if one of the following holds:*

- $p \not\equiv 7 \pmod{9}$ and $d \equiv (p+2)/3 \pmod{p-1}$; or
- $p \not\equiv 4 \pmod{9}$ and $d \equiv (2p+1)/3 \pmod{p-1}$; or
- $p = 19$ and $d \equiv 5$ or $11 \pmod{18}$.

Proof. The conditions on p and d imply that $p \geq 7$ and $d \geq 5$. And we may assume that $d < p-1$ by replacing it with its remainder upon division by $p-1$. We shall use Lemma 2.9 to bound $V_{F, d}$. Let $\text{wt} = \text{wt}_{p,1}$ be the p -ary weight function on $\mathbb{Z}/(p-1)\mathbb{Z}$ as defined in (4), and note that for any $a \in \mathbb{Z}/(p-1)\mathbb{Z}$, the value of $\text{wt}(a)$ is equal to the unique integer in $\{0, 1, \dots, p-2\}$ that is congruent to a modulo $p-1$. We use the convention that if $z \in \mathbb{Z}$, then $\text{wt}(z)$ is a shorthand for $\text{wt}(\bar{z})$, where $\bar{z} \in \mathbb{Z}/(p-1)\mathbb{Z}$ is the reduction modulo $p-1$ of z .

Now write $u = p-1$ and note that $u/6$ is an integer since $p \equiv 1 \pmod{6}$ and $u \geq 6$ because $p \geq 7$. Write $u = da + r$ with a positive integral quotient a and remainder $r \in \{1, \dots, d-1\}$, so then $a = (u-r)/d$. Then $r \equiv -da \pmod{u}$, and so

$$\text{wt}(a) + \text{wt}(-da) = \text{wt}(a) + \text{wt}(r) = a + r = \frac{u-r}{d} + r.$$

Lemma 2.9 will prove our desired bound ($V_{F, d} \leq 1/3$) if we show that

$$\frac{u-r}{d} + r \leq \frac{u}{3},$$

which is equivalent to

$$(d-1)r \leq (d-3)\frac{u}{3}.$$

If we have $d < (u/3) - 2$, then since $r \leq d-1$ and $d \geq 5$, we have $(d-1)r \leq (d-1)^2 \leq (d-3)(d+3) \leq (d-3)(u/3)$, which means that our inequality is satisfied, and equality is not actually possible (we would need $d = 5$ and $u/3 = d+3$, which would force $u = 24$, that is, $p = 25$, which is absurd).

We cannot have $d = (u/3) - 2$, since that would make d even, hence not coprime to u .

If we have $d = (u/3) - 1$, then note that $p \geq 19$ since we have $d \geq 5$. Furthermore, we have $-3d \equiv 3 \pmod{u}$, so then

$$\text{wt}(3) + \text{wt}(-3d) = 3 + 3 = 6,$$

and this is less than or equal to $u/3$ because $p \geq 19$ (with equality only when $p = 19$ and $d = 5$).

We cannot have $d = u/3$, for then $\gcd(d, u) = u/3 > 1$.

If we have $(u/3) + 1 \leq d < u/2$, then $a = 2$ and $r = u - 2d$, so then $\text{wt}(a) + \text{wt}(r) = 2 + u - 2d \leq u/3$ with equality if and only if $d = (u/3) + 1 = (p+2)/3$.

We cannot have $d = u/2$, for then $\gcd(d, u) = u/2 > 1$.

We cannot have $d = (u/2) + 1 = (p+1)/2$, because we are assuming $d \not\equiv 1 \pmod{(p-1)/2}$.

If we have $(u/2) + 2 \leq d < 2u/3$, then write $d = (u/2) + e$, so that $2 \leq e < u/6$. And write $u - d = 2eb + s$ with $0 \leq s < 2e$, so that $b = \frac{(u/2) - e - s}{2e} \leq \frac{u}{8} - \frac{1}{2}$. Since $2d \equiv 2e \pmod{u}$, we have $-d(2b+1) \equiv -2be - d \equiv s \pmod{u}$, and then

$$\text{wt}(2b+1) + \text{wt}(-d(2b+1)) = \text{wt}(2b+1) + \text{wt}(s) = 2b+1+s$$

because $2b+1 \leq \frac{u}{4} = \frac{p-1}{4} < p-1$ and $s < 2e < \frac{u}{3} = \frac{p-1}{3} < p-1$. So to prove our upper bound on $V_{\mathbb{F}_p, d}$ it suffices to show that $2b+1+s \leq u/3$, that is,

$$\frac{(u/2) - s}{e} + s \leq \frac{u}{3},$$

or equivalently,

$$(e-1)s \leq (2e-3)\frac{u}{6}.$$

This is in fact always satisfied: since $s \leq 2e-1$ and $2 \leq e < \frac{u}{6}$, we have $(e-1)s \leq (e-1)(2e-1) \leq (2e-3)(e+1) \leq (2e-3)(u/6)$, and we can only have exact equality if $2 = e = (u/6) - 1$, that is, if $p = 19$ and $d = (u/2) + e = 11$.

We cannot have $d = 2u/3$, for then $\gcd(d, u) = u/3 > 1$.

If we have $d \geq (2u/3) + 1$, then $a = 1$ and $r = u - d$ and $\text{wt}(a) + \text{wt}(r) = 1 + u - d \leq u/3$, with exact equality only if $d = (2u/3) + 1 = (2p+1)/3$.

Thus we have proved our upper bound on $V_{\mathbb{F}_p, d}$ for all values of d , and have shown that equality can be achieved only if $d = (u/3) + 1 = (p+2)/3$ or $d = (2u/3) + 1 = (2p+1)/3$ or else if $p = 19$ and $d \in \{5, 11\}$. For the former two cases, Lemmata 5.6 and 5.7 tell us precisely when $\gcd(d, p-1) = 1$, and show that $V_{\mathbb{F}_p, d} = 1/3$ in these cases. And it is easy to check that $V_{\mathbb{F}_{19}, 5} = V_{\mathbb{F}_{19}, 11} = 1/3$ by direct computation of the value m from Lemma 2.9. \square

Proposition 5.3. *Let F be a prime field of order p with p odd and $p \equiv 2 \pmod{3}$. If d is a positive integer with $\gcd(d, p-1) = 1$ and $d \not\equiv 1 \pmod{(p-1)/2}$, then $V_{F, d} \leq \frac{p+1}{3(p-1)}$. Equality is achieved if and only if one of the following holds:*

- $d \equiv 3 \pmod{p-1}$, or
- $d \equiv (2p-1)/3 \pmod{p-1}$.

Proof. The conditions on p and d imply that $p \geq 5$ and $d \geq 3$. If $d = 3$, then Lemma 5.8 below shows that $V_{\mathbb{F}_p,3} = (p+1)/(3(p-1))$. So we assume that $d \geq 5$ henceforth. And we may assume that $d < p-1$ by replacing it with its remainder upon division by $p-1$. We shall use Lemma 2.9 to bound $V_{F,d}$. Let $\text{wt} = \text{wt}_{p,1}$ be the p -ary weight function on $\mathbb{Z}/(p-1)\mathbb{Z}$ as defined in (4), and note that for any $a \in \mathbb{Z}/(p-1)\mathbb{Z}$, the value of $\text{wt}(a)$ is equal to the unique integer in $\{0, 1, \dots, p-2\}$ that is congruent to a modulo $p-1$. We use the convention that if $z \in \mathbb{Z}$, then $\text{wt}(z)$ is a shorthand for $\text{wt}(\bar{z})$, where $\bar{z} \in \mathbb{Z}/(p-1)\mathbb{Z}$ is the reduction modulo $p-1$ of z .

Now write $u = p-1$ and note that $(u+2)/6$ is an integer since $p \equiv 5 \pmod{6}$ and $u \geq 4$ because $p \geq 5$. Write $u = da + r$ with a positive integral quotient a and remainder $r \in \{1, \dots, d-1\}$, so then $a = (u-r)/d$. Then $r \equiv -da \pmod{u}$, and so

$$\text{wt}(a) + \text{wt}(-da) = \text{wt}(a) + \text{wt}(r) = a + r = \frac{u-r}{d} + r.$$

Lemma 2.9 will prove our desired bound ($V_{F,d} \leq \frac{p+1}{3(p-1)} = \frac{u+2}{3(p-1)}$) if we show that

$$\frac{u-r}{d} + r \leq \frac{u+2}{3},$$

which is equivalent to

$$(d-1)r - 2 \leq (d-3)\frac{u+2}{3}.$$

If we have $d < (u-1)/3$, then since $r \leq d-1$ and $d \geq 5$, we have $(d-1)r - 2 \leq (d-1)^2 - 2 \leq (d-3)(d+2) \leq (d-3)(u+2)/3$, which means that our inequality is satisfied, and equality is not actually possible. (We would need $d+2 = (u+2)/3$, which would make d even, hence not coprime to $p-1$.)

If we have $d = (u-1)/3$, then note that $p \geq 17$ since we have $d \geq 5$. Furthermore, we have $-3d \equiv 1 \pmod{u}$, so then

$$\text{wt}(3) + \text{wt}(-3d) = 3 + 1 = 4,$$

and this is strictly less than $(u+2)/3$ since $p \geq 17$.

If we have $(u+2)/3 \leq d < u/2$, then $a = 2$ and $r = u - 2d$, so then $\text{wt}(a) + \text{wt}(r) = 2 + u - 2d \leq (u+2)/3$ and we could only get equality if $d = (u+2)/3 = (p+1)/3$, but this is impossible, since it would make d even, hence not coprime to u .

We cannot have $d = u/2$, for then $\gcd(d, u) = u/2 > 1$.

We cannot have $d = (u/2) + 1 = (p+1)/2$, because we are assuming $d \not\equiv 1 \pmod{(p-1)/2}$.

If $(u/2) + 2 \leq d \leq 2(u-1)/3$, then write $d = (u/2) + e$, so that $2 \leq e \leq (u-4)/6$. And write $u - d = 2eb + s$ with $0 \leq s < 2e$, so that

$b = \frac{(u/2)-e-s}{2e}$. Note that $b \leq \frac{u}{8} - \frac{1}{2}$. Since $2d \equiv 2e \pmod{p-1}$, we have $-d(2b+1) \equiv -2be - d \equiv s \pmod{p-1}$. Thus

$$\text{wt}(2b+1) + \text{wt}(-d(2b+1)) = \text{wt}(2b+1) + \text{wt}(s) = 2b+1+s,$$

since $2b+1 \leq \frac{u}{4} = \frac{p-1}{4} < p-1$ and $s < 2e \leq (u-4)/3 = (p-5)/3 < p-1$. So to prove our upper bound, it suffices to show that $2b+1+s \leq (u+2)/3$, that is,

$$\frac{(u/2)-s}{e} + s \leq \frac{u+2}{3},$$

or equivalently,

$$(e-1)s - 1 \leq (2e-3)\frac{u+2}{6}.$$

This is in fact always satisfied strictly: since $s \leq 2e-1$ and $2 \leq e \leq (u-4)/6$, we have $(e-1)s - 1 \leq (e-1)(2e-1) - 1 = (2e-3)e < (2e-3)(u+2)/6$.

If we have $d \geq (2u+1)/3$, then $a = 1$ and $r = u-d$, so $\text{wt}(a) + \text{wt}(r) = 1+u-d \leq (u+2)/3$, with equality possible only if $d = (2u+1)/3 = (2p-1)/3$.

Thus we have proved our upper bound on $V_{\mathbb{F}_p, d}$ for all values of d , and have shown that equality can be achieved only if $d = 3$ or $(2p-1)/3$. And Lemma 5.8 shows that in both of these cases we have $\gcd(d, p-1) = 1$ and $V_{\mathbb{F}_p, d} = (p+1)/(3(p-1))$. \square

Proposition 5.4. *Let p be a prime with $p \equiv 1 \pmod{4}$ and $p \geq 13$, let F be the finite field of order p^2 , and let d be a positive integer with $d \equiv (p+1)/2 \pmod{p-1}$ and $\gcd(d, p^2-1) = 1$. Then $V_{F, d} \leq 1/2$.*

Proof. We can assume that $d < p^2-1$ by replacing d with the remainder one gets when one divides it by p^2-1 . Then we can write $d = \frac{p+1}{2} + b(p-1)$ for some b with $0 < b \leq p$. (We cannot have $b = 0$, for then we would have $\gcd(d, p^2-1) \geq \gcd(d, p+1) = \frac{p+1}{2} > 1$.)

We shall use Lemma 2.9 to bound $V_{F, d}$. Let $\text{wt} = \text{wt}_{p, 2}$ be the p -ary weight function on $\mathbb{Z}/(p^2-1)\mathbb{Z}$ as defined in (4). We use the convention that if $z \in \mathbb{Z}$, then $\text{wt}(z)$ is a shorthand for $\text{wt}(\bar{z})$, where $\bar{z} \in \mathbb{Z}/(p^2-1)\mathbb{Z}$ is the reduction modulo p^2-1 of z .

If $b = 1$, then $d = (3p-1)/2$. Then note that $-(p+4)d = \frac{-3p^2-11p+4}{2} \equiv \frac{p-11}{2} \cdot p \pmod{p^2-1}$, so that

$$\text{wt}(p+4) + \text{wt}(-d(p+4)) = 5 + \frac{p-11}{2} = \frac{p-1}{2},$$

and so $V_{F, d} \leq 1/2$ by Lemma 2.9

If $1 < b < (p-1)/2$, then $d = \frac{(2b+1)p-(2b-1)}{2}$. Then note that $-(p+2)d = \frac{-(2b+1)p^2-(2b+3)p+(4b-2)}{2} \equiv \frac{p^2-(2b+3)p+(2b-4)}{2} \equiv b-2+p \cdot \frac{p-2b-3}{2} \pmod{p^2-1}$, so that

$$\text{wt}(p+2) + \text{wt}(-d(p+2)) = 3 + b - 2 + \frac{p-2b-3}{2} = \frac{p-1}{2},$$

and so $V_{F, d} \leq 1/2$ by Lemma 2.9.

If $b = (p-1)/2$, then $d = 1 + p \cdot \frac{p-1}{2}$, and so $pd = p + p^2 \cdot \frac{p-1}{2} \equiv p + \frac{p-1}{2} \equiv \frac{3p-1}{2} \pmod{p^2-1}$, and we have shown (in the $b = 1$ case) that $V_{F,pd} \leq 1/2$, so then $V_{F,d} \leq 1/2$ by Remark 2.2.

We cannot have $b = (p+1)/2$, for then $\gcd(d, p^2-1) \geq \gcd(d, p+1) \geq (p+1)/2 > 1$.

If $(p+1)/2 < b \leq p$, then $d = \frac{(2b+1)p-(2b-1)}{2}$, so $-d = \frac{-(2b+1)p+(2b-1)}{2} \equiv \frac{(2p-2b-1)p+(2b-3)}{2} \equiv (p-b)p + \frac{2b-(p+3)}{2} \pmod{p^2-1}$, so that

$$\text{wt}(1) + \text{wt}(-d) = 1 + p - b + \frac{2b-(p+3)}{2} = \frac{p-1}{2},$$

and so $V_{F,d} \leq 1/2$ by Lemma 2.9. \square

Lemma 5.5. *Let p be odd and let $d = (q+1)/2$. Then $d \equiv 1 \pmod{p-1}$ if and only if n is even. We have $\gcd(d, q-1) = 1$ if and only if $q \equiv 1 \pmod{4}$, in which case $V_{F,d} = n/2$.*

Proof. First of all, $d = \frac{(p-1)}{2}(1 + p + \cdots + p^{n-1}) + 1$, so $d \equiv 1 + n \cdot \frac{p-1}{2} \equiv 1 \pmod{p-1}$ if and only if $2 \mid n$.

Secondly, $\gcd(d, q-1) = \gcd(d, q-1-2d) = \gcd(d, -2)$ and $2 \mid d$ if and only if $4 \mid q+1$, that is, if and only if $q \equiv 3 \pmod{4}$.

We assume that $\gcd(d, q-1) = 1$ henceforth, and determine $V_{F,d}$ via Lemma 2.9. Let $\text{wt} = \text{wt}_{p,n}$ be the p -ary weight function on $\mathbb{Z}/(p^n-1)\mathbb{Z}$ as defined in (4). Suppose a is chosen among the nonzero $x \in \mathbb{Z}/(p^n-1)\mathbb{Z}$ that minimize $\text{wt}(x) + \text{wt}(-dx)$, and among such x , make sure that a is one with $\text{wt}(a)$ minimal. Then we claim that $\text{wt}(a) \leq 2$ because otherwise there is some nonzero $a' = a - p^j - p^k$ such that $\text{wt}(a') = \text{wt}(a) - 2$, and then note that since p is odd and $d-1 = (q-1)/2$, we have $-da' = -da + (p^j + p^k)(q-1)/2 + p^j + p^k = -da + p^j + p^k$, so that $\text{wt}(-da') \leq \text{wt}(-da) + 2$, and so $\text{wt}(a') + \text{wt}(-da') \leq \text{wt}(a) + \text{wt}(-da)$.

If $\text{wt}(a) = 2$, say $a = p^j + p^k$, then $-da = -(p^j + p^k)(q-1)/2 - p^j - p^k = -p^j - p^k = -a$, so then $\text{wt}(a) + \text{wt}(-da) = n(p-1)$. But if $\text{wt}(a) = 1$, then $a = p^i$ for some i , so that $\text{wt}(-da) = \text{wt}(-d) = n(p-1)/2 - 1$, and so $\text{wt}(a) + \text{wt}(-da) = n(p-1)/2$. So

$$\min_{\substack{a \in \mathbb{Z}/(p^n-1)\mathbb{Z} \\ a \neq 0}} \text{wt}_{p,n}(a) + \text{wt}_{p,n}(-da) = \frac{n(p-1)}{2},$$

and so Lemma 2.9 shows that $V_{F,d} = n/2$. \square

Finally, we prove more results used in the proofs of Propositions 5.2 and 5.3.

Lemma 5.6. *Let $p \equiv 1 \pmod{3}$ and $d = (q+2)/3$. Then $d \equiv 1 \pmod{p-1}$ if and only if $3 \mid n$. We have $\gcd(d, q-1) = 1$ if and only if $q \pmod{9} \in \{1, 4\}$, in which case $V_{F,d} = n/3$.*

Proof. First of all, $d = \frac{p-1}{3}(1 + p + \cdots + p^{n-1}) + 1$, so $d \equiv 1 + n \cdot \frac{p-1}{3} \equiv 1 \pmod{p-1}$ if and only if $3 \mid n$.

Secondly, $\gcd(d, q-1) = \gcd(d, q-1-3d) = \gcd(d, -3)$ and $3 \mid d$ if and only if $9 \mid q+2$, that is, if and only if $q \equiv 7 \pmod{9}$.

We assume that $\gcd(d, q-1) = 1$ henceforth, and determine $V_{F,d}$ via Lemma 2.9. Let $\text{wt} = \text{wt}_{p,n}$ be the p -ary weight function on $\mathbb{Z}/(p^n-1)\mathbb{Z}$ as defined in (4). Suppose a is chosen among the nonzero $x \in \mathbb{Z}/(p^n-1)\mathbb{Z}$ that minimize $\text{wt}(x) + \text{wt}(-dx)$, and among such x , make sure that a is one with $\text{wt}(a)$ minimal. Then we claim that $\text{wt}(a) \leq 3$ because otherwise there is some nonzero $a' = a - p^j - p^k - p^\ell$ such that $\text{wt}(a') = \text{wt}(a) - 3$, and then note that since $p \equiv 1 \pmod{3}$ and $d-1 = (q-1)/3$, we have $-da' = -da + (p^j + p^k + p^\ell)(q-1)/3 + p^j + p^k + p^\ell = -da + p^j + p^k + p^\ell$, so that $\text{wt}(-da') \leq \text{wt}(-da) + 3$, and so $\text{wt}(a') + \text{wt}(-da') \leq \text{wt}(a) + \text{wt}(-da)$. So $\text{wt}(a) = 1, 2$, or 3 .

If $\text{wt}(a) = 3$, say $a = p^j + p^k + p^\ell$, then $-da = -(p^j + p^k + p^\ell)(q-1)/3 - p^j - p^k - p^\ell = -p^j - p^k - p^\ell$ since $p \equiv 1 \pmod{3}$. So $-da = -a$, and so $\text{wt}(a) + \text{wt}(-da) = n(p-1)$.

If $\text{wt}(a) = 1$, say $a = p^i$, then $\text{wt}(-da) = \text{wt}(-d) = \text{wt}(2(q-1)/3 - 1) = 2n(p-1)/3 - 1$, and so $\text{wt}(a) + \text{wt}(-da) = 2n(p-1)/3$.

If $\text{wt}(a) = 2$, say $a = p^j + p^k$, then $-da = -(p^j + p^k)(q-1)/3 - p^j - p^k$ and since $p \equiv 1 \pmod{3}$, this means $p^j + p^k - da = (q-1)/3$. So $n(p-1)/3 = \text{wt}(p^j + p^k - da) \leq 2 + \text{wt}(-da) = \text{wt}(a) + \text{wt}(-da)$. And in fact, if we just pick $a = 2$, then $\text{wt}(-da) = \text{wt}((q-1)/3 - 2) = n(p-1)/3 - 2$, so that $\text{wt}(a) + \text{wt}(-da) = n(p-1)/3$. So

$$\min_{\substack{a \in \mathbb{Z}/(p^n-1)\mathbb{Z} \\ a \neq 0}} \text{wt}_{p,n}(a) + \text{wt}_{p,n}(-da) = \frac{n(p-1)}{3},$$

and so Lemma 2.9 shows that $V_{F,d} = n/3$. \square

Lemma 5.7. *Let $p \equiv 1 \pmod{3}$ and $d = (2q+1)/3$. Then $d \equiv 1 \pmod{p-1}$ if and only if $3 \mid n$. We have $\gcd(d, q-1) = 1$ if and only if $q \pmod{9} \in \{1, 7\}$, in which case $V_{F,d} = n/3$.*

Proof. First of all, $d = \frac{2(p-1)}{3}(1 + p + \dots + p^{n-1}) + 1$, so $d \equiv 1 + 2n \cdot \frac{p-1}{3} \equiv 1 \pmod{p-1}$ if and only if $3 \mid n$.

Secondly, since d is odd we have $\gcd(d, q-1) = \gcd(d, 2q-2) = \gcd(d, 2q-2-3d) = \gcd(d, -3)$ and $3 \mid d$ if and only if $9 \mid 2q+1$, that is, if and only if $q \equiv 4 \pmod{9}$.

We assume that $\gcd(d, q-1) = 1$ henceforth, and determine $V_{F,d}$ via Lemma 2.9. Let $\text{wt} = \text{wt}_{p,n}$ be the p -ary weight function on $\mathbb{Z}/(p^n-1)\mathbb{Z}$ as defined in (4). Suppose a is chosen among the nonzero $x \in \mathbb{Z}/(p^n-1)\mathbb{Z}$ that minimize $\text{wt}(x) + \text{wt}(-dx)$, and among such x , make sure that a is one with $\text{wt}(a)$ minimal. Then we claim that $\text{wt}(a) \leq 3$ because otherwise there is some nonzero $a' = a - p^j - p^k - p^\ell$ such that $\text{wt}(a') = \text{wt}(a) - 3$, and then note that since $p \equiv 1 \pmod{3}$ and $d-1 = 2(q-1)/3$, we have $-da' = -da + 2(p^j + p^k + p^\ell)(q-1)/3 + p^j + p^k + p^\ell = -da + p^j + p^k + p^\ell$, so

that $\text{wt}(-da') \leq \text{wt}(-da) + 3$, and so $\text{wt}(a') + \text{wt}(-da') \leq \text{wt}(a) + \text{wt}(-da)$. So $\text{wt}(a) = 1, 2$, or 3 .

If $\text{wt}(a) = 3$, say $a = p^j + p^k + p^\ell$, then $-da = -2(p^j + p^k + p^\ell)(q-1)/3 - p^j - p^k - p^\ell = -p^j - p^k - p^\ell$ since $p \equiv 1 \pmod{3}$. So $-da = -a$, and so $\text{wt}(a) + \text{wt}(-da) = n(p-1)$.

If $\text{wt}(a) = 2$, say $a = p^j + p^k$, then $-da = -2(p^j + p^k)(q-1)/3 - p^j - p^k$ and since $p \equiv 1 \pmod{3}$, this means $p^j + p^k - da = 2(q-1)/3$. So $2n(p-1)/3 = \text{wt}(p^j + p^k - da) \leq 2 + \text{wt}(-da) = \text{wt}(a) + \text{wt}(-da)$.

If $\text{wt}(a) = 1$, say $a = p^i$, then $\text{wt}(-da) = \text{wt}(-d) = \text{wt}((q-1)/3 - 1) = n(p-1)/3 - 1$, and so $\text{wt}(a) + \text{wt}(-da) = n(p-1)/3$. So

$$\min_{\substack{a \in \mathbb{Z}/(p^n-1)\mathbb{Z} \\ a \neq 0}} \text{wt}_{p,n}(a) + \text{wt}_{p,n}(-da) = \frac{n(p-1)}{3},$$

and so Lemma 2.9 shows that $V_{F,d} = n/3$. \square

Lemma 5.8. *Let p be odd and $p \equiv 2 \pmod{3}$. Then $3 \not\equiv 1 \pmod{p-1}$. We have $\gcd(3, q-1) = 1$ if and only if $q \equiv 2 \pmod{3}$, in which case the multiplicative inverse of 3 modulo $q-1$ is $d = (2q-1)/3$ and $V_{F,3} = V_{F,d} = n \cdot \frac{p+1}{3(p-1)}$, and $d \not\equiv 1 \pmod{p-1}$.*

Proof. First of all, since p is odd and congruent to 2 modulo 3, we have $p \geq 5$, so $3 \not\equiv 1 \pmod{p-1}$.

Secondly, it is clear that $\gcd(3, q-1) = 1$ if and only if $q \not\equiv 1 \pmod{3}$, and since q is a power of p (which is not 3), this is true if and only if $q \equiv 2 \pmod{3}$.

We assume that $\gcd(3, q-1) = 1$ henceforth and set $d = (2q-1)/3$. Then $3d = 2q-1 \equiv 1 \pmod{q-1}$, so d is the multiplicative inverse of 3 modulo $q-1$. So $3d \equiv 1 \pmod{p-1}$ and since $3 \not\equiv 1 \pmod{p-1}$, this means that $d \not\equiv 1 \pmod{p-1}$.

Since 3 and d are inverses of each other modulo $q-1$, Remark 2.3 tells us that $V_{F,3} = V_{F,d}$, so it remains to show that $V_{F,3} = n(p+1)/3$, which we now do using Lemma 2.9. Let $\text{wt} = \text{wt}_{p,n}$ be the p -ary weight function on $\mathbb{Z}/(p^n-1)\mathbb{Z}$ as defined in (4). Suppose a is chosen among the nonzero $x \in \mathbb{Z}/(q-1)\mathbb{Z}$ that minimize $\text{wt}(x) + \text{wt}(-3x)$, and among such x , make sure that a is one with $\text{wt}(a)$ minimal. Write $a = a_0 + a_1p + \cdots + a_{n-1}p^{n-1}$ with $0 \leq a_i < p$ for each i , and at least one a_i is nonzero, and at least one a_i is not $p-1$. If $a_i \geq (p+1)/3$ for some i , let $a' = a - p^i(p+1)/3$, so that $\text{wt}(a') = \text{wt}(a) - (p+1)/3$. Note that $-3a' = -3a + (p+1)p^i$, so that $\text{wt}(-3a') \leq \text{wt}(-3a) + 2$, and thus $\text{wt}(a') + \text{wt}(-3a') \leq \text{wt}(a) + \text{wt}(-3a) - (p+1)/3 + 2 \leq \text{wt}(a) + \text{wt}(-3a)$, and since $\text{wt}(a') < \text{wt}(a)$, this would contradict our choice of a unless $a' = 0$. And if $a' = 0$, then $a = p^i(p+1)/3$, so then $-3a = -p^i(p+1) = -p^{i+1} - p^i$ and so $\text{wt}(a) + \text{wt}(-3a) = (p+1)/3 + n(p-1) - 2 \geq n(p-1)$, and this would contradict the choice of a since $\text{wt}(1) + \text{wt}(-3) = 1 + n(p-1) - 3 < n(p-1)$.

So we must have $a_i \leq (p-2)/3$ for every i , and thus $3a_i \leq p-2$ for every i . So $3a = 3a_0 + 3a_1p + \cdots + 3a_{n-1}p^{n-1}$ has $\text{wt}(3a) = 3\text{wt}(a)$, and

so $\text{wt}(a) + \text{wt}(-3a) = \text{wt}(a) + n(p-1) - \text{wt}(3a) = n(p-1) - 2\text{wt}(a)$. And since $a_i \leq (p-2)/3$ for every i , we have $\text{wt}(a) \leq n(p-2)/3$, and so $\text{wt}(a) + \text{wt}(-3a) \geq n(p+1)/3$, with equality if we let every $a_i = (p-2)/3$, that is, let $a = (p-2)(q-1)/(3(p-1))$. So

$$\min_{\substack{a \in \mathbb{Z}/(p^n-1)\mathbb{Z} \\ a \neq 0}} \text{wt}_{p,n}(a) + \text{wt}_{p,n}(-3a) = \frac{n(p+1)}{3},$$

and so Lemma 2.9 shows that $V_{F,3} = n(p+1)/(3(p-1))$. \square

6. OPEN PROBLEMS

Theorem 3.1 gives us a universal bound $V_{F,d} \leq (2/3)[F : \mathbb{F}_p]$ when d is nondegenerate over F . When $[F : \mathbb{F}_p]$ is a multiple of 3, Lemma 3.2 says that this universal bound is always attained for some d . Remark 1.2 furnishes a stronger bound of $V_{F,d} \leq (1/2)[F : \mathbb{F}_p]$ when $[F : \mathbb{F}_p] = 2^s$ with $s \geq 1$ and d is nondegenerate over F , and for each such F , this stronger bound is always attained for some d by Lemma 4.2 (except when $F = \mathbb{F}_4$, over which there is no nondegenerate d). When F is a prime field \mathbb{F}_p and d is nondegenerate over F (which requires $p \geq 5$), Theorem 5.1 gives upper bounds of $V_{F,d} \leq 1/2$ when $p \equiv 1 \pmod{4}$, and $V_{F,d} \leq \lceil (p-1)/3 \rceil / (p-1)$ when $p \equiv 3 \pmod{4}$, and Lemmata 5.5–5.8 show that these bounds are always met for some d in every such F .

So it remains to determine precisely how high $V_{F,d}$ can be when $[F : \mathbb{F}_p]$ is neither a power of 2 nor a multiple of 3. If ℓ is the least odd prime divisor of $[F : \mathbb{F}_p]$, then Lemma 3.2 shows that there is some d such that $V_{F,d} = \frac{\ell+1}{2\ell}[F : \mathbb{F}_p]$. We are unaware of any pair (F, d) where this value is exceeded. Thus we make the following conjecture that the value of $V_{F,d}$ observed in Lemma 3.2 is in fact the upper bound.

Conjecture 6.1 (Upper Bound Conjecture). *Suppose that $[F : \mathbb{F}_p]$ is not a power of 2, and let ℓ be the least odd prime divisor of $[F : \mathbb{F}_p]$. Let d be a positive integer with $\gcd(d, q-1) = 1$ that is not degenerate over F . Then $V_{F,d} \leq \frac{\ell+1}{2\ell}[F : \mathbb{F}_p]$.*

This bound coincides with the universal bound $V_{F,d} \leq (2/3)[F : \mathbb{F}_p]$ when $\ell = 3$, but is often stronger when $\ell > 3$. Computer checks have verified Conjecture 6.1 for all fields F of order less than 10^{13} .

Again consider our universal bound $V_{F,d} \leq (2/3)[F : \mathbb{F}_p]$ for d nondegenerate over F . It is interesting that the proof (in Section 3) does not use Stickelberger's Theorem (which underlies Lemma 2.9). Attempts to prove the universal bound directly with Stickelberger's Theorem lead to an interesting conjecture in elementary number theory that, if true, would provide an alternative proof for the universal bound. To state the conjecture, recall that if t is an integer with $t \geq 2$ and n is a positive integer, then we define the standard t -ary expansion of an $a \in \mathbb{Z}/(t^n - 1)\mathbb{Z}$ to be the expression

$$a = a_0 t^0 + a_1 t^1 + \cdots + a_{n-1} t^{n-1},$$

where the powers of t are elements of $\mathbb{Z}/(t^n - 1)\mathbb{Z}$ and a_0, \dots, a_{n-1} are elements of \mathbb{Z} with $0 \leq a_i < t$ for every i , and where we insist that $a_0 = \dots = a_n = 0$ when $a = 0$ (to make the a_i 's uniquely defined). If $b \in \mathbb{Z}/(t^n - 1)\mathbb{Z}$ has standard t -ary expansion $b = b_0 + b_1t + \dots + b_{n-1}t^{n-1}$, then we say that b covers a and write $a \preceq b$ to indicate that $a_i \leq b_i$ for every i . If $a \preceq b$ and $a \neq b$, we say that b strictly covers a and write $a \prec b$.

Conjecture 6.2 (Covering Conjecture). *Let t be an integer with $t \geq 2$ and let n and d be positive integers such that d modulo $t^n - 1$ is neither zero nor a power of t . Then there exist nonzero $a, b \in \mathbb{Z}/(t^n - 1)\mathbb{Z}$ such that $a \prec b$ and $db \prec da$.*

To see that this conjecture would provide an alternative proof of our universal bound (Theorem 3.1), let d be a positive integer coprime to $p^n - 1$ and nondegenerate over F . Then Conjecture 6.2 would show that there are nonzero $a, b \in \mathbb{Z}/(p^n - 1)\mathbb{Z}$ such that $a \prec b$ and $db \prec da$. Let $\text{wt} = \text{wt}_{p,n}$ be the p -ary weight function for $\mathbb{Z}/(p^n - 1)\mathbb{Z}$ as defined in (4). Now we shall use Stickelberger's Theorem via Lemma 2.9: since a , $-b$, and $b - a$ are all nonzero elements of $\mathbb{Z}/(p^n - 1)\mathbb{Z}$, we will obtain our universal bound $V_{F,d} \leq 2n/3$ if we can prove that at least one of $\alpha = \text{wt}(-da) + \text{wt}(a)$, $\beta = \text{wt}(db) + \text{wt}(-b)$ or $\gamma = \text{wt}(da - db) + \text{wt}(b - a)$ is less than or equal to $(2/3)n(p-1)$. Since b covers a , when we add a and $b - a$ to obtain b , there are no carries (in base p representation), so $\text{wt}(a) + \text{wt}(b - a) = \text{wt}(b)$. And thus $\text{wt}(a) + \text{wt}(b - a) + \text{wt}(-b) = \text{wt}(b) + \text{wt}(-b) = n(p-1)$. Similarly, we have $\text{wt}(db) + \text{wt}(da - db) + \text{wt}(-da) = n(p-1)$. Thus $\alpha + \beta + \gamma = 2n(p-1)$ and so at least one of the three summands is less than or equal to $(2/3)n(p-1)$.

We have considerable evidence for the truth of Conjecture 6.2. To see this, we first provide some observations and partial proofs. The first observation shows that one only needs to check the conjecture for bases t that are not powers of smaller integers.

Remark 6.3. If Conjecture 6.2 is true when $t = t_1$ and $n = n_1$, then it is also true when $t = t_1^k$ and $n = n_1/k$ for any positive divisor k of n_1 . For if $x \prec y$ when x and y are expressed in standard t_1 -ary expansions, then $x \prec y$ when they are expressed in standard (t_1^k) -ary expansions.

The second observation is that Conjecture 6.2 is trivial when d is not coprime to $t^n - 1$.

Lemma 6.4. *Let t , n , and d be positive integers with $t \geq 2$ and $1 < \gcd(d, t^n - 1) < t^n - 1$. Then there exist nonzero $a, b \in \mathbb{Z}/(t^n - 1)\mathbb{Z}$ such that $a \prec b$ and $db \prec da$.*

Proof. Let $e = (t^n - 1) / \gcd(d, t^n - 1)$, so that $1 < e = \gcd(e, t^n - 1) < t^n - 1$ and $de \equiv 0 \pmod{t^n - 1}$. Let $\bar{e} \in \mathbb{Z}/(t^n - 1)\mathbb{Z}$ be the reduction of e modulo $t^n - 1$. This e is neither zero nor a power of t modulo $t^n - 1$, so there exists some k such that $t^k \prec \bar{e}$. And dt^k is a nonzero element of $\mathbb{Z}/(t^n - 1)\mathbb{Z}$ because $\gcd(dt^k, t^n - 1) = \gcd(d, t^n - 1) < t^n - 1$. Thus $d\bar{e} = 0 \prec dt^k$. \square

There is a useful principle for lifting instances of covering to higher moduli.

Lemma 6.5. *Let t, m, n , and d be positive integers with $t \geq 2$ and $m \mid n$. Suppose that there are nonzero $a, b \in \mathbb{Z}/(t^m - 1)\mathbb{Z}$ such that $a \prec b$ and $db \prec da$ in $\mathbb{Z}/(t^m - 1)\mathbb{Z}$. Then there are nonzero $A, B \in \mathbb{Z}/(t^n - 1)\mathbb{Z}$ such that $A \prec B$ and $dB \prec dA$ in $\mathbb{Z}/(t^n - 1)\mathbb{Z}$.*

Proof. Let g be the integer $(t^n - 1)/(t^m - 1)$ and let A, B be the unique elements of $\mathbb{Z}/(t^n - 1)\mathbb{Z}$ given by $A = ga$ and $B = gb$. (The fact that a and b are well defined modulo $t^m - 1$ makes ga and gb well defined modulo $t^n - 1$.) Then the t -ary expansion of A in $\mathbb{Z}/(t^n - 1)\mathbb{Z}$ is just the (n/m) -fold repetition of the t -ary expansion of a in $\mathbb{Z}/(t^m - 1)\mathbb{Z}$, and similarly with B relative to b , dA relative to da , and dB relative to db . So $A \prec B$ and $dB \prec dA$. \square

When d is invertible modulo $t^n - 1$, the conclusion of Conjecture 6.2 can often be deduced from direct examination of the standard t -ary expansions of $d \pmod{t^n - 1}$ and its multiplicative inverse.

Lemma 6.6. *Let t be an integer with $t \geq 2$ and let n and d be positive integers with $\gcd(d, t^n - 1) = 1$ and d not a power of t modulo $t^n - 1$. Let $\bar{d} \in \mathbb{Z}/(t^n - 1)\mathbb{Z}$ be the reduction of d modulo $t^n - 1$, and let \bar{e} be the multiplicative inverse of \bar{d} . Suppose that \bar{d} and \bar{e} have standard t -ary expansions $\bar{d} = d_0 + d_1t + \cdots + d_{n-1}t^{n-1}$ and $\bar{e} = e_0 + e_1t + \cdots + e_{n-1}t^{n-1}$, respectively, and there exist some $j, k \in \mathbb{Z}/n\mathbb{Z}$ with $j + k \equiv 0 \pmod{n}$ such that $d_j \neq 0$ and $e_k \neq 0$. Then $t^k \prec \bar{e}$ and $d\bar{e} \prec dt^k$.*

Proof. It is clear that $t^k \preceq \bar{e}$ because $e_k \neq 0$. And in fact $\bar{e} \neq t^k$, because then its inverse would be t^{n-k} , but we were given that d is not a power of t modulo $t^n - 1$. So $t^k \prec \bar{e}$.

The t -ary digits of dt^k are obtained by cyclically shifting those of \bar{d} , so that the j th digit of \bar{d} (which is nonzero) becomes the 0th digit of dt^k . Thus $d\bar{e} = 1 \preceq dt^k$. And $1 \neq dt^k$ because that would make $\bar{d} = t^{n-k}$, and d is not a power of t modulo $t^n - 1$. \square

These principles allow us to prove that Conjecture 6.2 becomes true if we add $d \not\equiv 1 \pmod{t-1}$ as an hypothesis.

Lemma 6.7. *Let t, n , and d be positive integers with $t \geq 2$, $d \not\equiv 0 \pmod{t^n - 1}$, and $d \not\equiv 1 \pmod{t-1}$. Then there exist nonzero $a, b \in \mathbb{Z}/(t^n - 1)\mathbb{Z}$ such that $a \prec b$ and $db \prec da$.*

Proof. We may assume $\gcd(d, t^n - 1) = 1$ because otherwise Lemma 6.4 guarantees our result. Then the hypotheses of Lemma 6.6 are clearly satisfied when $n = 1$, thus establishing our result in that case. Then the cases with $n > 1$ can be deduced from the $n = 1$ case along with Lemma 6.5. \square

And we also can prove Conjecture 6.2 when $n \leq 4$.

Lemma 6.8. *Let t and n be integers with $t \geq 2$ and $n \leq 4$, and let d be a positive integer such that d is neither zero nor a power of t modulo $t^n - 1$. Then there exist nonzero $a, b \in \mathbb{Z}/(t^n - 1)\mathbb{Z}$ such that $a \prec b$ and $db \prec da$.*

Proof. We may assume that $\gcd(d, t^n - 1) = 1$, because otherwise Lemma 6.4 gives us our result immediately. Without loss of generality we assume that $d < t^n - 1$ by replacing it with its remainder upon division by $t^n - 1$, and write $d = d_0 + \cdots + d_{n-1}t^{n-1}$ with $0 \leq d_i < t$ for each d_i . In view of Lemma 6.7, we may assume that $d \equiv 1 \pmod{t-1}$, and so $d_0 + \cdots + d_n \equiv 1 \pmod{t-1}$. Since d is not a power of t modulo $t^n - 1$, this means that $d_0 + \cdots + d_n \geq t$. Thus at least two of the d_i 's are nonzero. And if we let e be the integer with $0 \leq e < t^n - 1$ such that $de \equiv 1 \pmod{t^n - 1}$, and write $e = e_0 + \cdots + e_{n-1}t^{n-1}$ with $0 \leq e_i < t$ for each e_i , then e is not a power of t modulo $t^n - 1$ and $e \equiv 1 \pmod{t-1}$, so that at least two of the e_i 's are nonzero. If $n \leq 3$, this means that the hypotheses of Lemma 6.6 are satisfied, and so our conclusion follows.

So we may assume $n = 4$ henceforth. If $d_0 + d_1 + d_2 + d_3 > t$, then the fact that $d_0 + d_1 + d_2 + d_4 \equiv 1 \pmod{t-1}$ forces $d_0 + d_1 + d_2 + d_3 \geq 2t - 1$, which makes at least three of the d_i 's nonzero, and since we already know that at least two of the e_i 's are nonzero, the hypotheses of Lemma 6.6 are satisfied, and so our conclusion follows. Similarly, if $e_0 + e_1 + e_2 + e_3 > t$, our conclusion will follow from Lemma 6.6. So we may assume $d_0 + d_1 + d_2 + d_3 = e_0 + e_1 + e_2 + e_3 = t$ henceforth.

We cannot have $d \equiv 0 \pmod{t^2 - 1}$, for we are assuming that $\gcd(d, t^4 - 1) = 1$, which would force $t^2 - 1 = 1$, which is absurd. If d is not a power of t modulo $t^2 - 1$, then by the $n = 2$ case of this lemma (which has already been established), we have some $a, b \in \mathbb{Z}/(t^2 - 1)\mathbb{Z}$ such that $a \prec b$ and $db \prec da$ in $\mathbb{Z}/(t^2 - 1)\mathbb{Z}$. Then Lemma 6.5 furnishes $A, B \in \mathbb{Z}/(t^4 - 1)\mathbb{Z}$ with $A \prec B$ and $dB \prec dA$ in $\mathbb{Z}/(t^4 - 1)\mathbb{Z}$, and we are done.

If d is a power of t modulo $t^2 - 1$, say $d \equiv t^k \pmod{t^2 - 1}$, then $e \equiv t^k \pmod{t^2 - 1}$ also. Since $d \equiv (d_3 + d_1)t + (d_2 + d_0) \pmod{t^2 - 1}$ is a power of t and $d_0 + d_1 + d_2 + d_3 = t$, we know that $(d_3 + d_1)t + (d_2 + d_0)$ is not the standard t -ary expansion of d modulo $t^2 - 1$. So we must have $\{d_3 + d_1, d_2 + d_0\} = \{0, t\}$, and similarly $\{e_3 + e_1, e_2 + e_0\} = \{0, t\}$. Furthermore, since $d \equiv e \pmod{t^2 - 1}$, we either have $d_3 + d_1 = e_3 + e_1 = t$ or $d_2 + d_0 = e_2 + e_0 = t$. Since all d_i 's and e_i 's are less than t , we know that either d_3, d_1, e_3, e_1 are all nonzero or else d_2, d_0, e_2, e_0 are all nonzero, and so the hypotheses of Lemma 6.6 are satisfied, and our conclusion follows. \square

In addition to these partial proofs, computer checks also verify Conjecture 6.2 for all t^n less than $3 \cdot 10^9$.

ACKNOWLEDGEMENTS

The first author thanks Pascal Véron and Alicia Weng for stimulating discussions on some of the topics in this paper. The authors thank an

anonymous reviewer for helpful comments and corrections that improved the paper.

REFERENCES

- [1] Y. Aubry, D. J. Katz, and P. Langevin. Cyclotomie des sommes de Weil binomiales. *C. R. Math. Acad. Sci. Paris*, 352(5):373–376, 2014.
- [2] Y. Aubry, D. J. Katz, and P. Langevin. Cyclotomy of Weil sums of binomials. *J. Number Theory*, 154:160–178, 2015.
- [3] E. ÇakÇak and P. Langevin. Power permutations in dimension 32. In *Sequences and their applications—SETA 2010*, volume 6338 of *Lecture Notes in Comput. Sci.*, pages 181–187. Springer, Berlin, 2010.
- [4] A. R. Calderbank, G. McGuire, B. Poonen, and M. Rubinstein. On a conjecture of Helleseht regarding pairs of binary m -sequences. *IEEE Trans. Inform. Theory*, 42(3):988–990, 1996.
- [5] A. Canteaut, P. Charpin, and H. Dobbertin. Couples de suites binaires de longueur maximale ayant une corrélation croisée à trois valeurs: conjecture de Welch. *C. R. Acad. Sci. Paris Sér. I Math.*, 328(2):173–178, 1999.
- [6] A. Canteaut, P. Charpin, and H. Dobbertin. Binary m -sequences with three-valued crosscorrelation: a proof of Welch’s conjecture. *IEEE Trans. Inform. Theory*, 46(1):4–8, 2000.
- [7] A. Canteaut, P. Charpin, and H. Dobbertin. Weight divisibility of cyclic codes, highly nonlinear functions on \mathbf{F}_{2^m} , and crosscorrelation of maximum-length sequences. *SIAM J. Discrete Math.*, 13(1):105–138, 2000.
- [8] L. Carlitz. A note on exponential sums. *Math. Scand.*, 42(1):39–48, 1978.
- [9] L. Carlitz. Explicit evaluation of certain exponential sums. *Math. Scand.*, 44(1):5–16, 1979.
- [10] P. Charpin. Cyclic codes with few weights and Niho exponents. *J. Combin. Theory Ser. A*, 108(2):247–259, 2004.
- [11] T. Cochrane and C. Pinner. Stepanov’s method applied to binomial exponential sums. *Q. J. Math.*, 54(3):243–255, 2003.
- [12] T. Cochrane and C. Pinner. Explicit bounds on monomial and binomial exponential sums. *Q. J. Math.*, 62(2):323–349, 2011.
- [13] R. S. Coulter. Further evaluations of Weil sums. *Acta Arith.*, 86(3):217–226, 1998.
- [14] H. Davenport and H. Heilbronn. On an exponential sum. *Proc. London Math. Soc.* (2), 41(6):449–453, 1936.
- [15] H. Dobbertin, T. Helleseht, P. V. Kumar, and H. Martinsen. Ternary m -sequences with three-valued cross-correlation function: new decimations of Welch and Niho type. *IEEE Trans. Inform. Theory*, 47(4):1473–1481, 2001.
- [16] T. Feng. On cyclic codes of length $2^{2^r} - 1$ with two zeros whose dual codes have three weights. *Des. Codes Cryptogr.*, 62(3):253–258, 2012.
- [17] R. Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions. *IEEE Trans. Inform. Theory*, 14(1):154–156, 1968.
- [18] T. Helleseht. Krysskorrelasjonsfunksjonen mellom maksimale sekvenser over $\text{GF}(q)$. Master’s thesis, Matematisk Institutt, Universitetet i Bergen, 1971.
- [19] T. Helleseht. Some results about the cross-correlation function between two maximal linear sequences. *Discrete Math.*, 16(3):209–232, 1976.
- [20] H. D. L. Hollmann and Q. Xiang. A proof of the Welch and Niho conjectures on cross-correlations of binary m -sequences. *Finite Fields Appl.*, 7(2):253–286, 2001.
- [21] X.-D. Hou. A note on the proof of Niho’s conjecture. *SIAM J. Discrete Math.*, 18(2):313–319, 2004.
- [22] A. A. Karatsuba. On estimates of complete trigonometric sums. *Mat. Zametki*, 1:199–208, 1967. Trans. in *Math. Notes* 1(2):133–139, 1967.

- [23] T. Kasami. Weight distribution formula for some class of cyclic codes. Technical report, Univ. Illinois, Urbana, 1966.
- [24] T. Kasami. The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes. *Information and Control*, 18:369–394, 1971.
- [25] T. Kasami, S. Lin, and W. W. Peterson. Some results on cyclic codes which are invariant under the affine group and their applications. *Information and Control*, 11:475–496, 1967.
- [26] D. J. Katz. Weil sums of binomials, three-level cross-correlation, and a conjecture of Helleseth. *J. Combin. Theory Ser. A*, 119(8):1644–1659, 2012.
- [27] D. J. Katz. Divisibility of Weil sums of binomials. *Proc. Amer. Math. Soc.*, 143(11):4623–4632, 2015.
- [28] D. J. Katz and P. Langevin. Proof of a conjectured three-valued family of Weil sums of binomials. *Acta Arith.*, 169(2):181–199, 2015.
- [29] D. J. Katz and P. Langevin. New open problems related to old conjectures by Helleseth. *Cryptogr. Commun.*, 8(2):175–189, 2016.
- [30] N. Katz and R. Livné. Sommes de Kloosterman et courbes elliptiques universelles en caractéristiques 2 et 3. *C. R. Acad. Sci. Paris Sér. I Math.*, 309(11):723–726, 1989.
- [31] H. D. Kloosterman. On the representation of numbers in the form $ax^2+by^2+cz^2+dt^2$. *Acta Math.*, 49(3-4):407–464, 1927.
- [32] G. Lachaud and J. Wolfmann. Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristique 2. *C. R. Acad. Sci. Paris Sér. I Math.*, 305(20):881–883, 1987.
- [33] S. Lang. *Cyclotomic fields I and II*, volume 121 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.
- [34] P. Langevin. *Les sommes de caractères et la formule de Poisson dans la théorie des codes, des séquences et des fonctions booléennes*. PhD thesis, Université de Toulon, 1999.
- [35] P. Langevin. Numerical projects page: Numerical experiments on power functions, 2007. <http://langevin.univ-tln.fr/project/spectrum>.
- [36] P. Langevin and P. Véron. On the non-linearity of power functions. *Des. Codes Cryptogr.*, 37(1):31–43, 2005.
- [37] G. Leander and P. Langevin. On exponents with highly divisible Fourier coefficients and conjectures of Niho and Dobbertin. In *Algebraic geometry and its applications*, volume 5 of *Ser. Number Theory Appl.*, pages 410–418. World Sci. Publ., Hackensack, NJ, 2008.
- [38] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997.
- [39] R. J. McEliece. Weight congruences for p -ary cyclic codes. *Discrete Math.*, 3:177–192, 1972.
- [40] G. McGuire. On certain 3-weight cyclic codes having symmetric weights and a conjecture of Helleseth. In *Sequences and their applications: proceedings of SETA '01*, Discrete Math. Theor. Comput. Sci. (Lond.), pages 281–295. Springer, London, 2002.
- [41] G. M. McGuire and A. R. Calderbank. Proof of a conjecture of Sarwate and Pursley regarding pairs of binary m -sequences. *IEEE Trans. Inform. Theory*, 41(4):1153–1155, 1995.
- [42] H. M. Trachtenberg. *On the cross-correlation functions of maximal linear sequences*. PhD thesis, University of Southern California, Los Angeles, 1970.
- [43] I. Vinogradov. Some trigonometrical polynomes and their applications. *C. R. Acad. Sci. URSS (N.S.)*, (6):254–255, 1933.
- [44] L. R. Welch. Trace mappings in finite fields and shift register cross-correlation properties. Technical report, Dept. Electrical Engineering, University of Southern California, Los Angeles, 1969.

DEPARTMENT OF MATHEMATICS, CALIFORNIA STATE UNIVERSITY, NORTHRIDGE,
UNITED STATES

INSTITUT DE MATHÉMATIQUES DE TOULON, UNIVERSITÉ DE TOULON, FRANCE

DEPARTMENT OF MATHEMATICS, CALIFORNIA STATE UNIVERSITY, NORTHRIDGE,
UNITED STATES

DEPARTMENT OF MATHEMATICS, CALIFORNIA STATE UNIVERSITY, NORTHRIDGE,
UNITED STATES